Remarks

Claims 1-3 have been cancelled without prejudice.

Claims 4, 6, 7 and 8 have been amended to correct typographical errors.

The examiner's rejection of claims 4 and 6-8, based on the term "responsive" is not fully understood. In each claim, the word responsive must be read in light of the other words in the claim. For example, in claims 4 and 6, the cipher devices are responsive to keys when they "encrypt or decrypt a digital signal". Likewise in Claims 7 and 8, the function units are responsive to key data blocks when they "provide another key data block."

Withdrawal of the 112 rejections and allowance of Claims 8-10 is requested.

Claim 4 is rejected as obvious over Candelore in view of Coutts on the basis that it is well known to use a fixed length set of keys. However, Claim 4 recites the limitation, *inter alia*, "effectively inhibiting the operation of the most downstream of the modulo operators in the block cipher device having the first key." As described in the specification, one way of doing this is to employ a second key composed of bits whose function is to enable or disable functions that are component steps in the cryptographic algorithm. Both Candelore and Coutts disclose the use of a conventional public key algorithms, i.e., Data Encryption Standard (DES) and the Rivest Shamir, Adlermann (RSA) algorithms, in which it is well known that symbols of a key block perform as operands to functions that are component steps in the cryptographic algorithm. Thus, rather than inhibiting the operation of the algorithms as claimed, the cited art discloses that the keys perform as operands to the functions of the algorithms. Reconsideration and

allowance of Claim 4 is requested.

Claim 5 is dependent from Claim 4 and therefore allowable with Claim 4 without regard to the further patentable limitations recited therein.

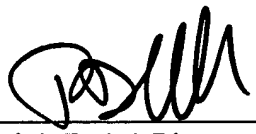
Claim 6 is rejected as obvious over Candelore in view of Coutts on the basis that it is well known to use a fixed length set of keys. However, Claim 6 recites the limitation, *inter alia*, of "combining the symbols provided by the two sections of the first key generator to cancel the symbols applied to a second stage." It is well understood by those of skill in the art, that the conventional public key algorithms disclosed in Coutts and Candelore do not operate in this fashion and thus the cited art does not provide a teaching of canceling symbols as claimed. Reconsideration and allowance of Claim 6 is requested.

Claim 7 is rejected as obvious over Candelore in view of Coutts in view of Lim on the basis that Lim teaches a key scheduler generating two subkeys. However, Claim 7 recites the limitation, *inter alia*, the specific operation of the key scheduler such that "the encryption stage will not encrypt data if the first portion of the key block data is equal to the second portion of the key data block, and the first function unit is equal to the second function unit." For example, when one of the component ciphers receives a variable that is the mod 2 addition of the upper and lower halves of the input combined key block, the upper and lower halves of the input combined key block are symmetric to each other, and that component cipher will always be keyed with an all zero variable. The contribution of that cipher to the overall algorithm calculation will therefore be negated. Lim does not

teach a key scheduler having the claimed operation. Reconsideration and allowance of Claim 7 is requested.

Allowance of Claims 4-10 is requested.

Respectfully submitted,



Patrick D. McPherson
Reg. No. 46,255
L. Lawton Rogers, III
Reg. No. 24,302
D. Joseph English
Reg. No. 42,514
Mark C. Comtois
Reg. No. 46,285

DUANE MORRIS LLP
1667 K Street, N.W., Suite 700
Washington, DC 20006
Telephone: (202) 776-7800
Facsimile: (202) 776-7801

Dated: June 24, 2005